MULTIPLE AUTHENTICATIONS IN A SYSTEM USING GRAPHICAL PASSWORD

Ansu Maria Varghese[1], Albin Varghese[2], Justin Sebastian[3] and Mrs. Jetty Benjamin[4]

[123] PG Scholars,Department of MCA, Amal Jyothi College of Engineering
[4]Assistant Professor, Department of MCA, Amal Jyothi College of Engineering

Abstarct: Graphical passwords give a promising option to conventional alphanumeric passwords. They are attractive since people usually remember pictures better than words. This paper proposes a password security system that allows the host not to store the passwords of its users at its end. Instead, it creates and stores an encrypted derivative of the password and a secret key with the help of images selected by the user during the user creation process. During the login attempts of users, the user is required to enter the password and secret key to select the same images. The proposed system verifies if the imaged during login matches with the original image that was provided during user creation by comparing their pixel information. Then, the system derives the password and secret key from the images with the help of the stored derivative. Then, the derived password is matched with the password entered by the user.

Keywords: Graphical authentication, image authentication, text password, dual authentication, 2-way authentication

I. INTRODUCTION

Authentication is the process of determining whether someone or something is, in fact, who or what it declares itself to be. Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server. Users are usually identified with a user ID, and authentication is accomplished when the user provides a credential, for example, a password, that matches with that user ID. Most users are most familiar with using a password, which, as a user, is called a knowledge authentication factor.

Secret phrase verification is the most broadly utilizing confirmation system for web applications. The majority of validation frameworks are utilizing the content based secret phrase. Serious issues in content-based passwords are overlooking secret word, stolen secret word, week secret key. Content-based passwords are helpless against different sorts of assaults like as savage power, spyware, and word reference. To conquer the vulnerabilities of content secret phrase, the graphical based secret key plan is proposed. In graphical secret key systems, pictures are used as passwords. The purpose of picking that technique is brain sciences ponder says that human personality recalls a great many pictures with detail. Customary validation relies upon the utilization of a secret word record, in which client IDs are put away together with hashes of the passwords related with every client. When signing in, the secret word put together by the client is hashed and contrasted with the incentive in the secret phrase record. In the event that the two hashes coordinate, the client is verified.

This way to deal with verification has a few downsides, especially for assets sent crosswise over various frameworks. For a certain something, assailants who can access to the secret word document for a framework can utilize savage power assaults against the hashed passwords to extricate the passwords. For another, this methodology would require different confirmations for current applications that get to assets over various frameworks. This approach to authentication has several drawbacks, particularly for resources deployed across different systems. For one thing, attackers who are able to access the password file for a system can use brute force attacks against the hashed passwords to extract the passwords. For another, this approach would require multiple authentications for modern applications that access resources across multiple systems.

II. LITERATURE REVIEW

Biswas et al [1], "Password Security system with 2-way authentication: A lot of pixels and a particular shading section are recognized by the calculation. The paired estimation of that shading portion of every pixel is changed over into decimal. The ASCII estimation of each character of the secret key is brought. The distinction in incentive between the ASCII esteem and the changed over decimal esteem is determined. The outcome is put away as a portion of the mystery key(or secret word) subordinate. We are utilizing even the arrangement of pixel estimations of the first picture for making the subordinate of the first segment of the password. The next segment of the secret phrase is contrasted and odd pixel estimations of the second image. Finally, for making mystery key subsidiary we are utilizing mixed(odd and even) pixel estimations of the third image. Likewise, every single other section for every one of the characters of mystery key is inferred.

Bhand et al[2], Enhancement of Password Authentication System Using Graphical Images: In this paper, the Enhancement of secret key confirmation framework with the assistance of pictures is proposed. This paper, for the most part, centers around the idea of graphical secret phrase framework. It is bolstered by the utilizing signaled click focuses for verification reason. The essential idea of this framework is just the association of the client with a succession of 5 pictures. The fundamental objective of this framework is to accomplish higher security with the basic procedure to use by a client and harder to figure by a programmer. The strategy utilizing is Cued Click Point framework upgraded with the versatile ready framework on potentially security strings. We are going to send a versatile alarm after the endeavor of hacking without knowing the program. For enlistment, the client can transfer his very own pictures nearly in any organization, or he/she can essentially choose a picture from the current database.At the season of enrollment, the client gets one framework created a content secret word on his email based on RGB estimations of the chose snap purposes of the picture. While signing in client needs to enter this content secret phrase and this content secret word is exceedingly verified on the second dimension by this signaled snap point method.While the program attempts to hack the framework after the third wrong click point one alarm message will be sent on clients portable to caution him.

Ms. Dhandha, et al[3],Enhancement of Password Authentication System Using Recognition based Graphical password for web Application:In this paper, it proposes recognition based graphical password scheme to provide security against spyware and shoulder surfing attacks as well as this scheme provide the two factor authentication in order to resist unauthorized users. In this scheme, at the time of sign up user has to choose images from a set of images given by the server and at the time of signing a user has to recognize that images from the set of images for authentication. It using random character set generation for each image to resist shoulder surfing as well as spyware attacks.It also fetches the user's password images randomly from the database to resist spyware attacks.

A) Sign up

In signup page 20 images are displayed on the screen that images are randomly fetched from the database. Show in the figure we are attaching a unique string on each image for resisting shoulder surfing as well as spyware attacks. The length of each string is three characters long. These strings are a combination of lowercase, an uppercase character, numbers, and special symbols. When the user has refreshed the page that time all images and string of each image are change. The user has to select a minimum three and maximum six images from 20 images by entering an appropriate string (which display on below right corner of each image) in the password field.

B) Signing

At the time of signing, the user has to enter the name that he or she used at the time of signup. If the user name valid then by pressing the tab key, the user's password images along with other images are fetching randomly from the database. A total of 12 images are displayed on the screen. In 12 images some of the images are user's password images. Suppose, at the time of sign up user has select three images as a password. During the signing process, the user's password images are fetching randomly from the database.

Ahsan, et al[4], Graphical Password Authentication utilizing Images Sequence: This paper proposes another procedure of client authentication that is Graphical Password Authentication using Images Sequence. In the existing condition, a significant issue in data security is client verification. There are numerous confirmation procedures like printed, graphical, biometric and so on. The current graphical confirmation methods dependent on picture choice are bad enough on the grounds that in these procedures pictures are predefined by the framework. In this paper, another procedure is proposed. In this technique, the client will transfer pictures from his/her own display/catalog for secret phrase determination and pictures transferred by one client won't be obvious to other clients. The succession of pictures is a key factor of the presented validation system. In this procedure the client will transfer pictures at the season of enrollment for secret key and for login, the client should choose the pictures which were transferred at the season of enlistment. Arrangement/request of pictures and number of pictures are a key factor of the proposed framework. Pictures transferred by one client are not unmistakable to other or unapproved clients.

Almulhem et al[5], A Graphical Password Authentication System: Alphanumerical passwords are required to fulfill two opposing prerequisites. They must be effectively recollected by a client, while they must be difficult to figure by an impostor. Clients are known to pick effectively guessable or potentially short content passwords, which are an obvious objective of word reference and beast constrained assaults. Authorizing a solid secret phrase strategy here and there prompts a contrary impact, as a client may turn to compose his or her hard to recall passwords on sticky notes presenting them to coordinate theft. In the writing, a few systems have been proposed to lessen the confinements of an alphanumerical secret key. One proposed arrangement is to utilize a simple to recall long expressions (passphrase) instead of a solitary word. Another proposed arrangement is to utilize graphical passwords, in which designs (pictures) are utilized rather than alphanumerical passwords. At theseason of enlistment, a client makes a graphical secret phrase by first entering an image the person picks. The client at that point picks a few point-of-intrigue (POI) areas in the image. Every POI is portrayed by a circle (focus and range). For each POI, the client types a word or expression that would be related to that POI. On the off chance that the client does not type any content in the wake of choosing a POI, at that point that POI is related with an unfilled string. For validation, the client first enters his or her username. The framework, at that point, shows the enlisted picture. The client, at that point, needs to accurately pick the POIs and type the related words. Whenever composed words either appear as bullets (*) or hidden. In this, a client uninhibitedly picks an image, POIs and relating words. The request and number of POIs can be authorized for more grounded validation.

III. METHODOLOGY

A. User Creation

The proposed system requires a new user to provide a text password,selection of three graphic images and a secret key while signing up along with a unique user name and other details. The set of pixels is used to prepare the password and secret key derivative.

- Creatingpassword derivative: The ASCII value of each character of the text password is compared against the decimal RGB value of a specific color segment of a specific pixel. The difference (= ASCII of character – the decimal value of color segment of a pixel) for each character of the user’s text password is stored as a distinct segment of the password derivative with the user record in an encrypted format to the host database.

- Creating secret derivative: The ASCII value of each character of the secret key is compared against the decimal RGB value of a specific color segment of a specific pixel. The difference (= ASCII of character – the decimal value of color segment of a pixel) for each character of the user’s secret key is stored as a distinct segment of the secret key derivative with the user record in an encrypted format to the host database.

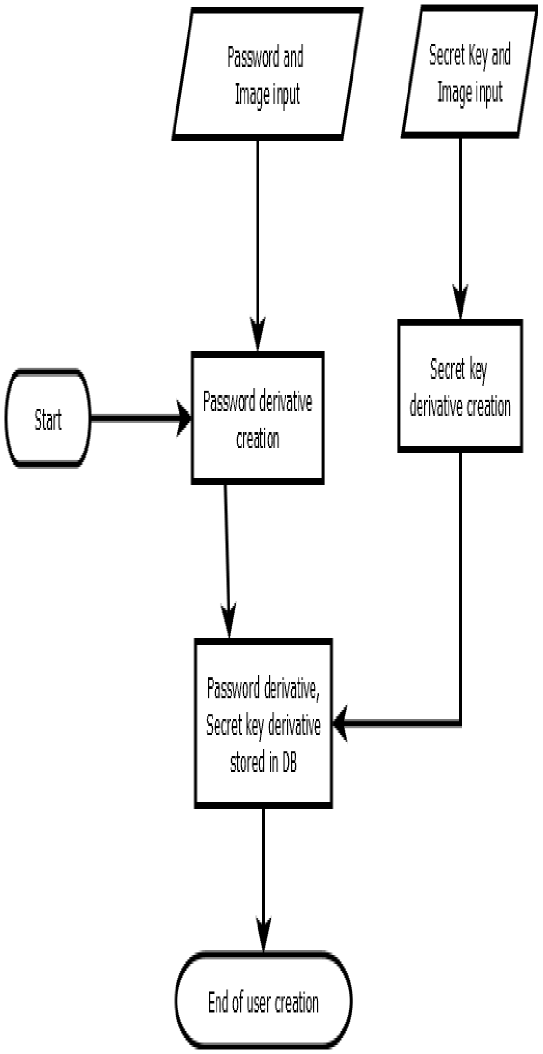
Password and Image input
Secret Key and Image input
Start
Password derivative creation
Secret key derivative creation
Password derivative, Secret key derivative stored in DB
End of user creation

Fig. 1. User creation process flowchart.

B. User verification

The proposed solution asks the users to enter the text password and select three images for a successful login. Once the required steps are completed, the image authentication is performed followed by the user authentication. The value stored in each segment of the password derivative is added or subtracted with or from the decimal value of a predefined color segment of the pixels. The resulting decimal values (considered as ASCII values) are converted into characters. The text formed by the characters is matched with the password(secret key) that is user entered. In the case of a match, the user is authenticated successfully.

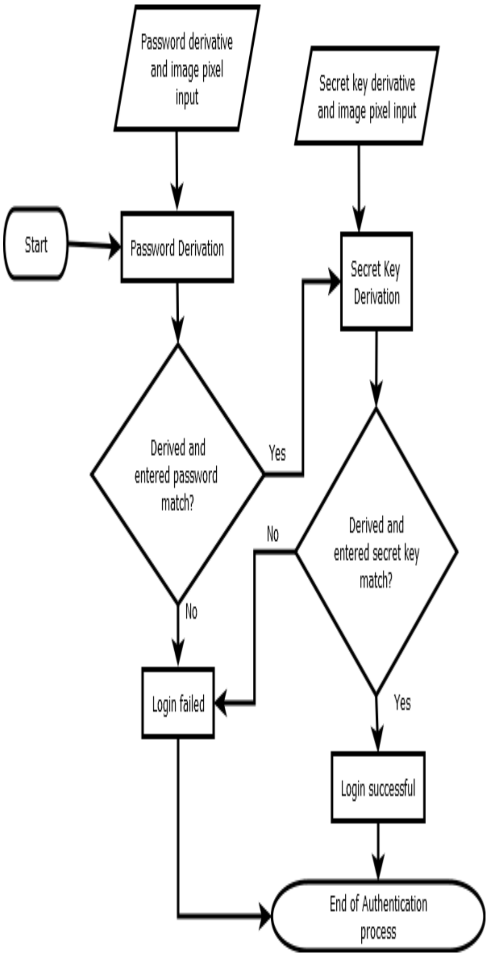
Password derivative and image pixel input
Secret key derivative and image pixel input
Start
Password Derivation
Secret Key Derivation
Derived and entered password match?
Yes
No
Derived and entered secret key match?
No
Yes
Login failed
Login successful
End of Authentication process

Fig. 2. Authentication process flowchart.

IV.IMPLEMENTATION

Generating Secret Keyand Password Derivative: A set of pixels and a specific color segment are identified by the algorithm. The binary value of that color segment of each pixel is converted into decimal. The ASCII value of each character of the password is fetched. The difference in value between the ASCII value and the converted decimal value is derived. The result is stored as a segment of a secret key(or password) derivative. We are using even set of pixel values of the first image for creating a derivative of the first section of the password. The next section of the password is compared with the odd pixel values of the second image. Finally, for creating a secret key derivative we are using mixed(odd and even) pixel values of the third image. Likewise, all other segments for all the characters of the secret key are derived.

- Generating ascii value of password

```
  $ascii[$i]=ord($cpwd[$i])
 ;
```

- Finding the RGB Value

```
  $color =
  imagecolorat($simgfrmjpg[1
  ],$i,$j);
  $rgb=imagecolorsforindex($
  simgfrmjpg[1],$color);

  $rgbtotal[$k1]=$rgb['red']
  +
  $rgb['green']+$rgb['blue']
  ;
```

- Substracting RGB Value-ASCII Value

```
  $sub1=array();

  for($i=0;$i<$len;$i++)
                  {

  $sub1[$i]=$ascii[$i]-
 $rgbtotal[$i];
                  }
```

- Checking Decrypted value for Authentication

```
       if(sizeof($rgbtotal)==sizeof
       ($a))
       $add1[$i]=$a[$i]+$rgbtotal[$
       i];

       if($add1[$i]==$ascii[$i]                                 }
{
       f=0;
       }
```

IV. RESULT

The proposed authentication system provides two layers of security. Hence, it is more resistant against unauthorized login attempts as compared to most of the authentication systems that rely solely on either text password or graphical authentication. The image authentication layer provides security against common hacking techniques like monitoring or recording users'keystrokes or attacks using shoulder-surfing and hidden cameras. In the proposed system, as the password is not stored anywhere and it is derived from the image the user is to provide during signing in, it mitigates the possibilities of user data security getting compromised in case of a host database hack.The solution can be implemented in any real-time online or offline applications to enable a robust password security mechanism. The drawback of this solution is it increases the complexity of the user authentication process. The users need to remember the alphanumeric text passwords along with the image used while signing in.

V. CONCLUSION

The proposed authentication system provides security over attacks by monitoring or recording users' keystrokes, shoulder surfing, and hidden camera. Even if the password is leaked and the host database is hacked, any random image cannot be modified accordingly as the sets of pixels (used in the authentication process) are identified by the algorithm. Thus, the pixel locations are not stored in the database. The unauthorized access cannot be prohibited if both the text password and the image are compromised. The user doesn't need to keep the image, handy for login.

VI. FUTURE WORK

The proposed authentication system provides security over attacks by monitoring or recording users' keystrokes, shoulder surfing, and hidden camera. In future it has great scope. It can be used everywhere instead of text-based password or can be used as high level security for text password also .We can increase the security of this system byincreasing the number of levels used. Presently there are many authentication system but they have their own advantages and disadvantages The security can be improved by adding more combination of image for authentication process. By adding more image combination we can divide the secret key also into two sections as we done with the password which enhances more security to the system. As how we have written over this system can be best alternative to the text password. It can be used almost everywhere like defence services, banking sectors and many more services to provide best password mechanism to user.

REFERENCES

[1] Subhradeep Biswas and Sudipa Biswas, "Password Security system with 2-way authentication", Third International Conference on

Research in Computational Intelligence and communication networks(ICRCICN),2017.

[2]Amol Bhand, Vaibhav Desale, Swati Shirke, Suvarna Pansambal Shirke, "Enhancement of password authentication system using graphical images", IEEE,2015.

[3]Ms.Dipti, H and Mr.Chandresh Parekh “Enhancement of Password Authentication System Using Recognition based Graphical password for Web Application", ISSN No. 0976-5697, Volume 8, No. 5, 2017.

[4] Muhammad Ahsan, Yugang Li et al[4], “Graphical Password Authentication utilizing Images Sequence”, International Research Journal of Engineering and Technology(IRJET),Volume:4,Nov-2017.

[5]Ahmad Almulhem, “A Graphical Password Authentication System”, IEEE,2011

.